Link Security for Aeronautical Wireless Networks

ICNS 2004

Simon Blake-Wilson, BCI
Kelly Mesveskas, FAA ACB-250
Vic Patel, FAA ACB-250

Goals

- Discuss whether link security for aeronautical wireless networks is a future NAS security requirement.
- Compare link security with security at other layers – e.g. application of end-to-end security.
- Investigate how link security can be provided.

Outline

- Is security for aeronautical wireless networks needed?
- Link security vs end-to-end security
- Link security requirements
- Likely link security approach
- Detailed example: link security for VDL Mode 3
- Conclusions

Is Wireless Security Needed?

Motivations for aeronautical wireless security include:

- Existing phantom controller phenomenon on analog voice ATC communications

Edition 5GN SUN 27 AUG 2000, Page News 1
Radio hackers steer aircraft into danger

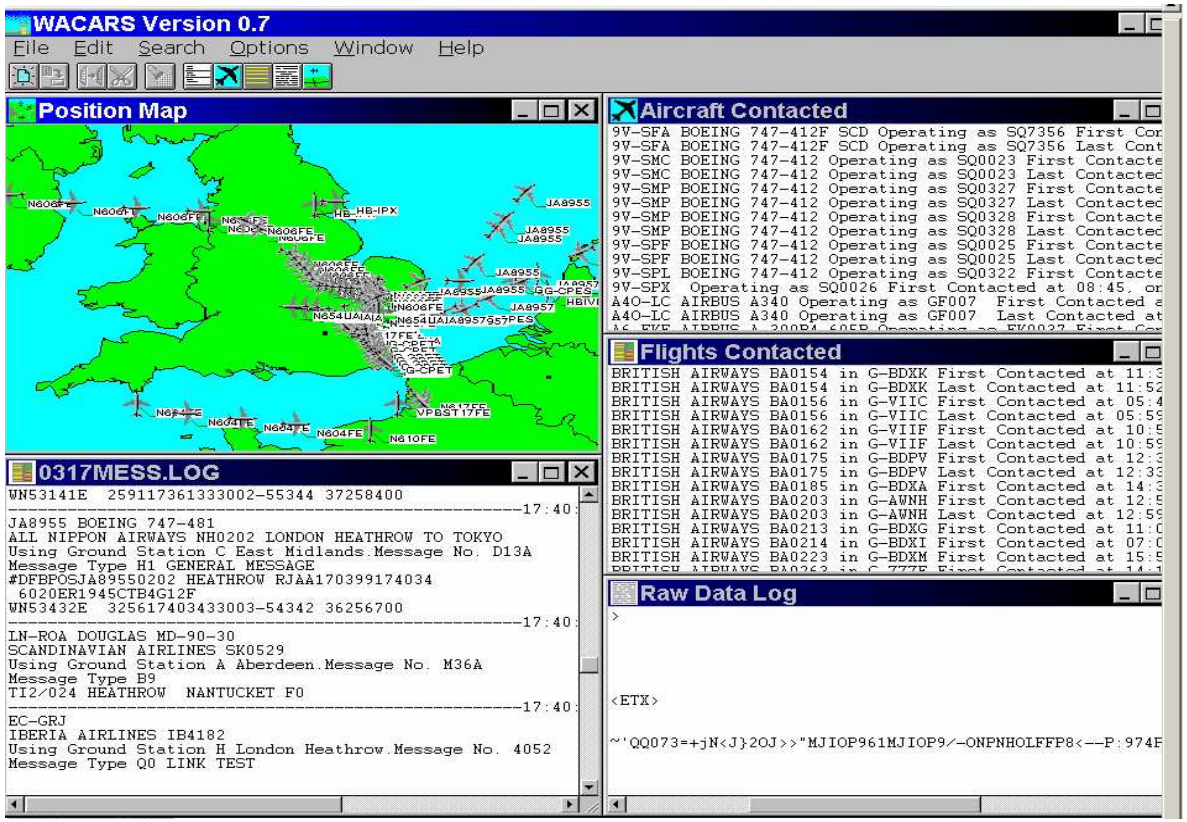
RADIO hackers posing as air traffic controllers are endangering hundreds of lives by giving bogus instructions to pilots as they take off and land.
A criminal investigation has been launched after one plane last month was twice given false instructions by a hoaxer as it approached a British airport. The Civil Aviation Authority (CAA) has issued a safety alert after 19 similar incidents in the past eight months.

Is Wireless Security Needed? (cont)

- Increase in attacks on other public safety wireless networks
  - Omaha, 2001 – hacker broadcasted rock song on police channel for 2 mins, interfering with negotiations with a man who was attempting to commit suicide
  - Minneapolis, 2000-1 – hacker broadcast misleading information on police, fire, and ambulance radios for almost 2 years
  - Scanner enthusiasts in DC post detailed logs of covert drug ops, movements of presidential aircraft at Edwards
  - Etc

Is Wireless Security Needed? (cont)

- Internet sites monitoring ACARS traffic



What's Disclosed?

- Graphical Position Reports
- Contact Reports
- Detailed Message Logs

Is Wireless Security Needed? (cont)

- Extreme interest in the media in the susceptibility of aeronautical wireless networks

Alaska Air Launches Wireless Check-in

Using free software on handhelds, travelers can check in, go directly to gate

Wireless LANs: Trouble in the Air

By Bob Brewin, Dan Verton and Jennifer DiSabatino
(Jan. 14, 2002) As the airline industry scrambles to meet a Jan. 18 deadline to screen every checked bag for explosives, security experts, analysts and government officials are raising serious concerns about the security of wireless technology that's integral to the effort.

Airport checks vulnerable to hackers, experts say

Carrie Kirby, Chronicle Staff Writer

Terrorist hackers could exploit wireless networks used to check baggage at major airports -- including San Jose's -- according to network security experts.

tion by airlines of industry-standard 802.11b, or Wi-Fi, wireless LANs
GHz band. These systems, which are widely viewed as inherently insecure,
ıpport such applications as bag matching and curbside and roving-agent

ar to be justified, based on two investigations that were conducted last week
ırity firms that analyzed airline wireless LAN systems at Denver International
e International Airport.

Is Wireless Security Needed? (cont)

- Ease of masquerade, modification, and replay attacks on unprotected RF networks
- Increased availability of attack tools as commercial technology is adopted in aeronautical wireless networks – WLAN, cellular, etc.
- Introduction of ATC data which precludes easy distinction between controllers and phantoms
- Introduction of unmanned aerial vehicles
- Increased automation of response to controller commands

Is Wireless Security Needed? (cont)

- Ubiquity of security in commercial wireless (and wired) networks
  - PPP – PAP, CHAP, EAP, etc
  - Ethernet and other wired IEEE 802 – 802.1x, EAP, etc
  - WLAN – WEP, 802.11i, etc
  - Bluetooth
  - Cellular networks – GSM, CDMA, TDMA

Link Security vs End-to-End Security

ATN Security Solution provides end-to-end, application layer security – isn't that enough?

- Link security protects just the air-ground link, application security protects end-to-end
- Link security protects more information in each packet
- Application security does not protect packets aimed at NAS penetration that are not addressed to secured end systems
- Combination of link security and application security common in commercial world
- Combination of link security and application security provides defense-in-depth

Link Security Requirements

Fundamental need to:

- Protect CAA's ground networks from intrusion
- Provide protection against phantom controllers

Link Security Requirements (cont)

Link security solutions typically based on 3 requirements:

- Initial entity authentication to make sure authorized parties are communicating
- Authentication of packets to prevent masquerade, modification, and replay
- Encryption of packets to prevent eavesdropping
  - Not appropriate in many ATC circumstances

Link Security Approach

Link security solutions will likely involve 3 components:

- Initial per-session entity authentication and session key establishment protocol
  - Symmetric key based
  - Public key based
- Data packet authentication using a MAC
- Voice packet authentication
  - Latency requirements and error handling create problems
  - Research required - non-cryptographic options?

VDL M3 Example: Basics

- VDL Mode 3 is a digital aeronautical wireless network that supports both voice and data
- XID exchange precedes data communications and is suitable for session establishment.
- No exchange suitable for session establishment precedes voice communications.
- XID exchange consists of air-ground then ground-air messages.
- XID messages include 256-byte signature field and are extensible.
- Data exchanges include an error detection field which could be replaced by a MAC.

VDL M3 Example: Options

A number of possible approaches for initial session authentication and key establishment:

- Symmetric: Kerberos
- Symmetric: Secure ID
- Symmetric: Cellular
- Public-key: Signatures
- Public-key: ATN

Each approach has pros and cons. We'll look in detail at the two most promising options: cellular and ATN.

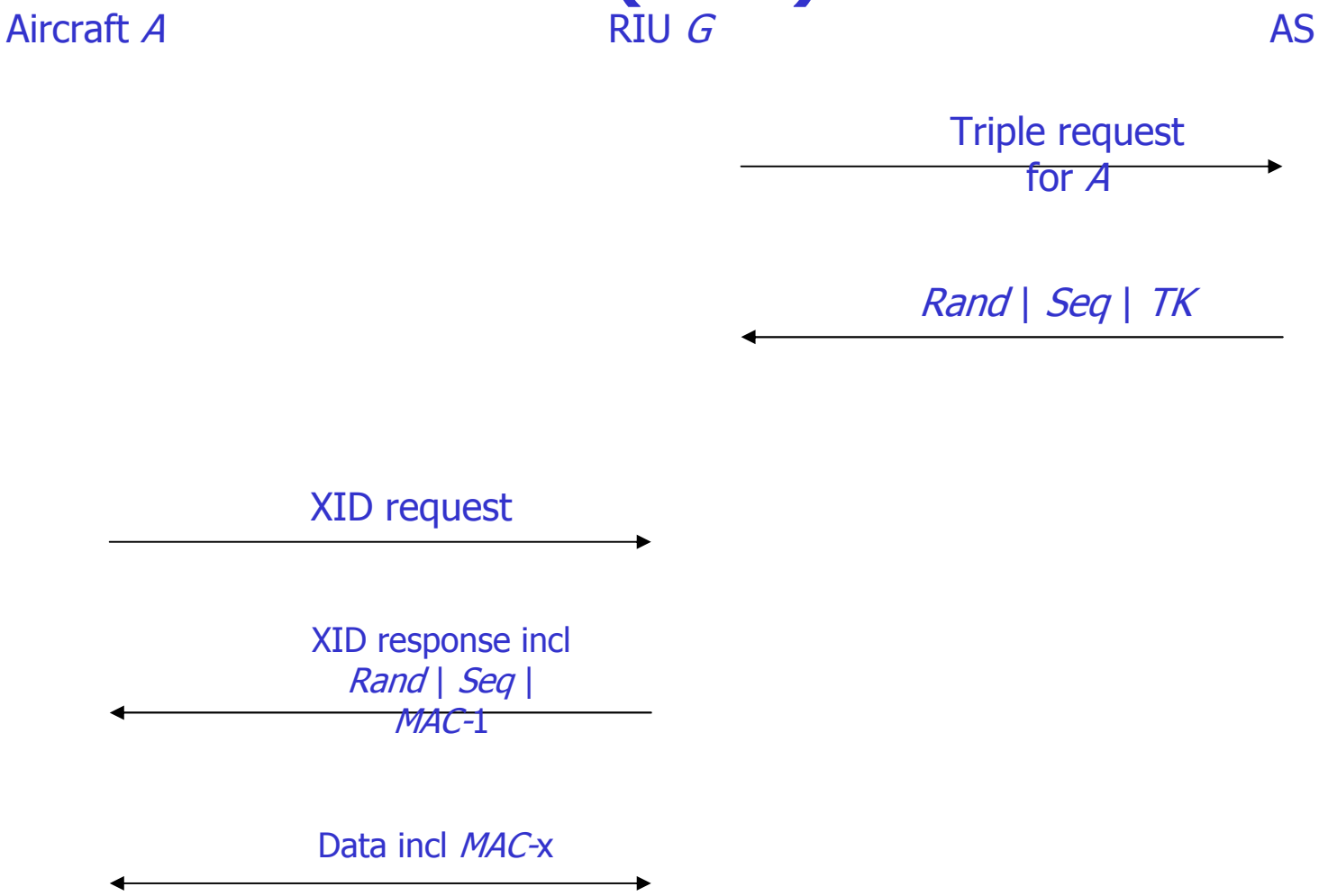
VDL M3 Example: Cellular Approach

Basics:

- Many variants of cellular security – GSM, CDMA, TDMA, CDMA2000, UMTS, etc
- All rely on secret shared between phones/SIM cards and central authority known as Authentication Center

Seems to have a number of nice features: handoff support, ground messaging can occur before logon, bandwidth minimized, support for multiple ACs and roaming built-in. Appears the best symmetric option.

VDL M3 Example: Cellular Approach (cont)



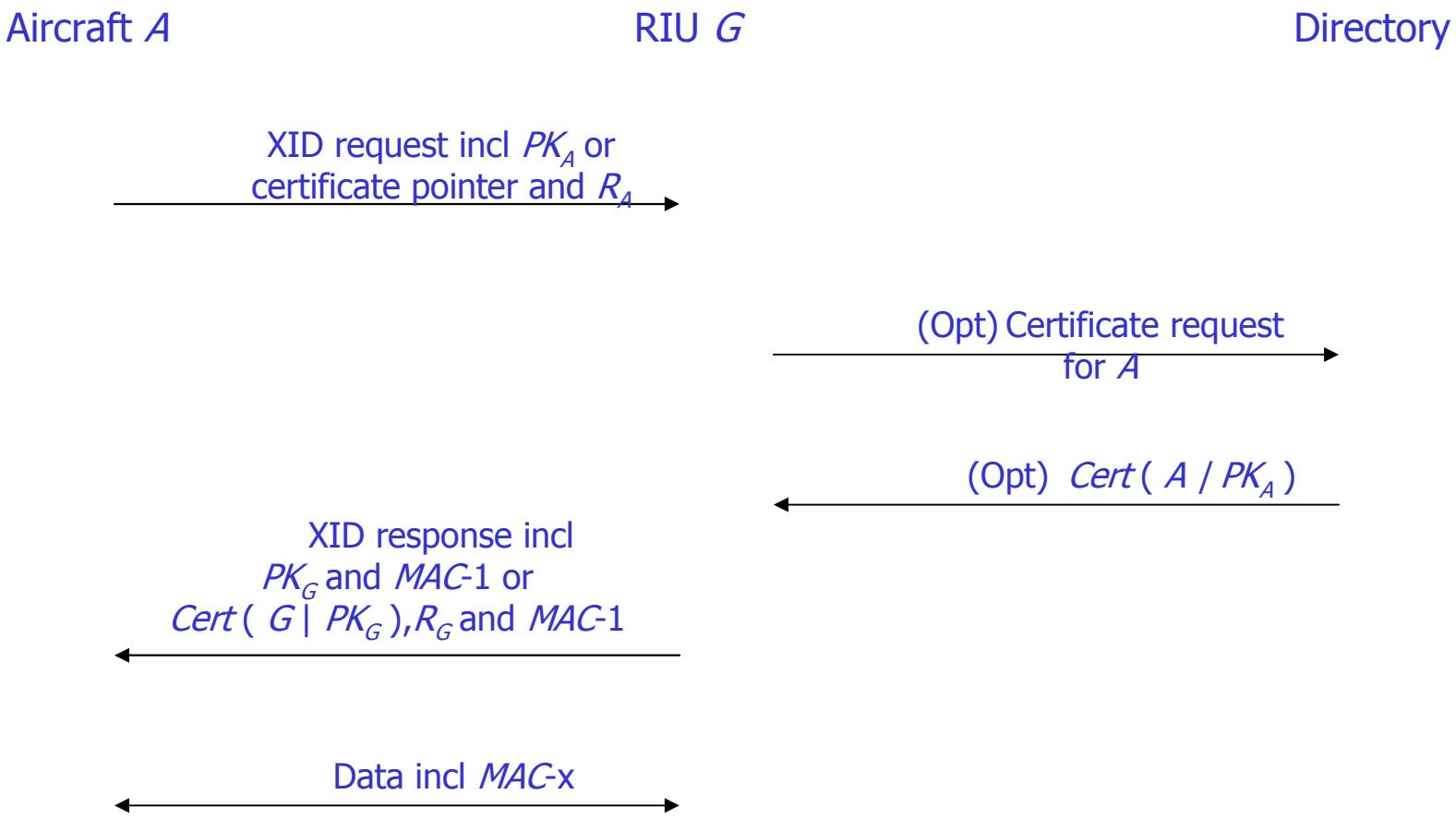
VDL M3 Example: ATN Approach

Basics:

- Integrate an authenticated key agreement protocol into the XID exchange
- Establish session keys which can be used with a MAC for authentication during and after the XID exchange

Seems to have a number of nice features: similarity to ATN approach to IDRP security and re-use of PKI, flexibility to support unilateral or mutual authentication. Appears most promising public-key based approach.

VDL M3 Example: ATN Approach (cont)



VDL M3 Example: Comparison

	Cellular Approach	**ATN Approach**
Infrastructure required	Authentication server which must be online 24/7 – higher maintenance cost	Certificate Authority and directory – higher set-up cost
Cryptographic overhead during XID exchange	Only symmetric cryptography operations required – less computation and bandwidth	Public-key cryptography operations required – some additional computation and bandwidth
Personalization required	Each aircraft must be personalized, no RIU personalization required.	Options to avoid need to personalize aircraft and RIUs depending on desired security properties
Commonality with ATN security	Different approach compared to ATN security	Commonality with ATN security – possible to use the same PKI for ATN security and VDL Mode 3 security
Security services provided	Mutual entity authentication followed by data authentication of all messages after the initial XID request	Mutual or unilateral entity authentication followed by data authentication of all messages after the initial XID request
Infrastructure network security required	Session keys are sent from the AS to the RIU – security required over the network	No infrastructure network security required.
Handoff support	Designed to support cellular handoff but unknown for VDL Mode 3	Unknown for VDL Mode 3

Conclusions

- Predicting the future is hard – history tells us that security threats develop in mysterious ways
- Predicting the future is important – deploying security on aeronautical wireless networks will take time
- There seems a clear possibility that aeronautical wireless networks will need security
- Sensible approach: (1) standardize security, (2) implement security, (3) deploy security – each step is beneficial whether the following steps occur or not
- Open technical problems exist that will require fundamental research – e.g. authentication of voice packets